

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Joint Workshop on Security Modeling ArchiMate Forum and Security Forum

Feltus, Christophe; Band, Iver

Publication date:
2012

[Link to publication](#)

Citation for pulished version (HARVARD):

Feltus, C & Band, I 2012, *Joint Workshop on Security Modeling ArchiMate Forum and Security Forum..*

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Joint Workshop on Security Modeling

ArchiMate Forum and Security Forum



Facilitators:

Erik Proper, Senior Research Manager and
Christophe Feltus, Senior Research Engineer,
Public Research Center Henri Tudor

Iver Band, Enterprise Architect,
Standard Insurance Company

Workshop Agenda

- Welcome and purpose
- Introductions
- Research spotlight: Strengthening RBAC with Responsibility Modeling
- Motivation: The *Inaction* Problem in Information Security
- Open Discussion:
 - Complementing TOGAF® and ArchiMate® with enhanced security modeling
 - Identification and prioritization of challenges
 - Next steps and adjourn

Workshop Purpose

- The acceptance and maturity of TOGAF and ArchiMate present opportunities to
 - Improve the conceptual and visual modeling of enterprise information security
 - Drive usage of TOGAF and ArchiMate for security architecture
 - Enable information security stakeholders to make *better decisions* about protecting their interests
 - Enable all business leaders to understand the impact of information security or the lack thereof
- We are here to identify and prioritize these opportunities, and to plan efforts to exploit them

Brief Personal Introductions

- Name
- Organization and position
- Involvement in The Open Group
- Security and modeling background and interests

Research Spotlight: Strengthening RBAC with Responsibility Modeling

The *Open Group* Conference,
San Francisco, USA, Feb 2, 2012

Sponsored by



Christophe Feltus
Senior R&D Engineer

Public Research Centre Henri Tudor
29, avenue John F. Kennedy
L-1855 Luxembourg-Kirchberg

Tel +352 42 59 91 - 1
Fax +352 42 59 91 - 777
www.tudor.lu

christophe.feltus@tudor.lu

Outline

- Context of the research
 - The problem / the research approach
 - What is RBAC ?
 - Case study
- 1st research question: How should responsibility be modelled, both in general and specifically in ArchiMate ?
- 2nd research question: How can models of responsibility be used to improve access rights management ?
- Conclusions

The Problem

The research addresses two problems arising from security and governance requirements, such as Basel II and Sarbanes-Oxley

- Enterprises must precisely provision access rights according to business needs, principles such as least privilege and separation of duties as well as statutory requirements.
 - RBAC partially solves that problem
 - Enterprises must precisely define responsibilities and stakeholders must understand them.
 - Today, there is no standard business definition of responsibility
- Both problems are linked: Responsibility definition enables precise provisioning of access rights

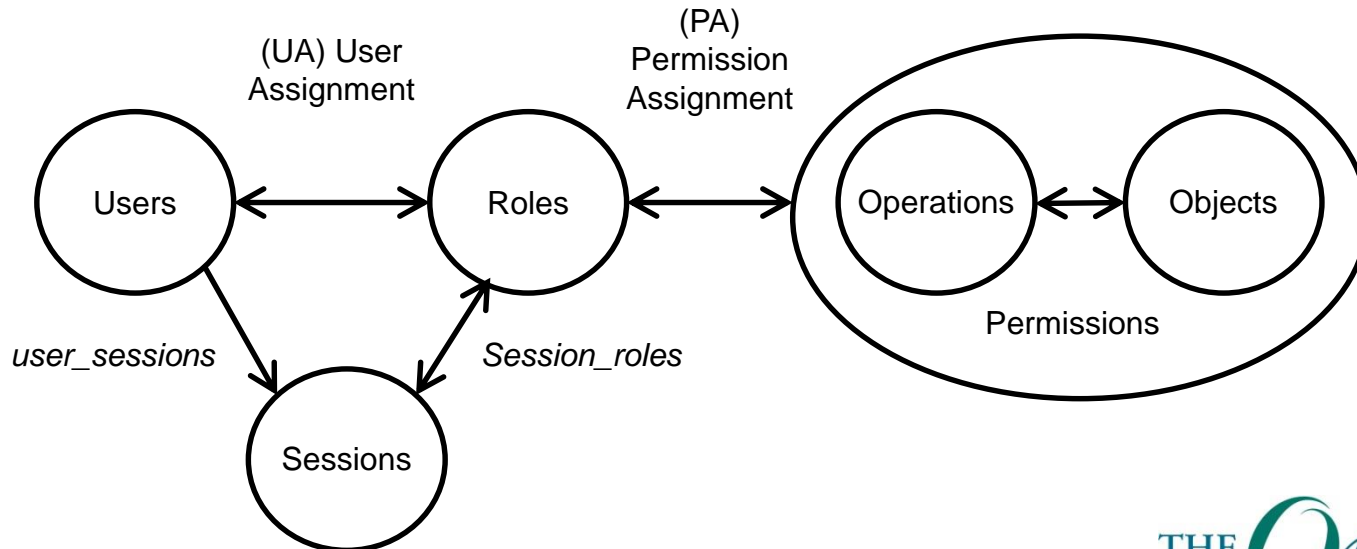
Approach

- In order to solve the problem:
 - We explore a model to define responsibilities
 - We consider access rights provisioning based on the model

RBAC

Modeling RBAC with SABSA, TOGAF and
ArchiMate, Creating a Foundation for
Understanding and Action,
Iver Band, CISSP
Open Group Conference, Austin, Texas

- A widely implemented mechanism for protecting system resources. Relies on user authentication, which in turn relies on identity management
- Defines and applies relationships between
 - Users – often human, but can also be systems
 - Roles – job functions defined for an organization
 - Permissions – organizational consent to perform specific operations
- Ensures that each user can execute only those operations authorized through roles that are both assigned to that user and activated for that user's session
- Four standard and cumulative levels (hierarchical, constraint,...)



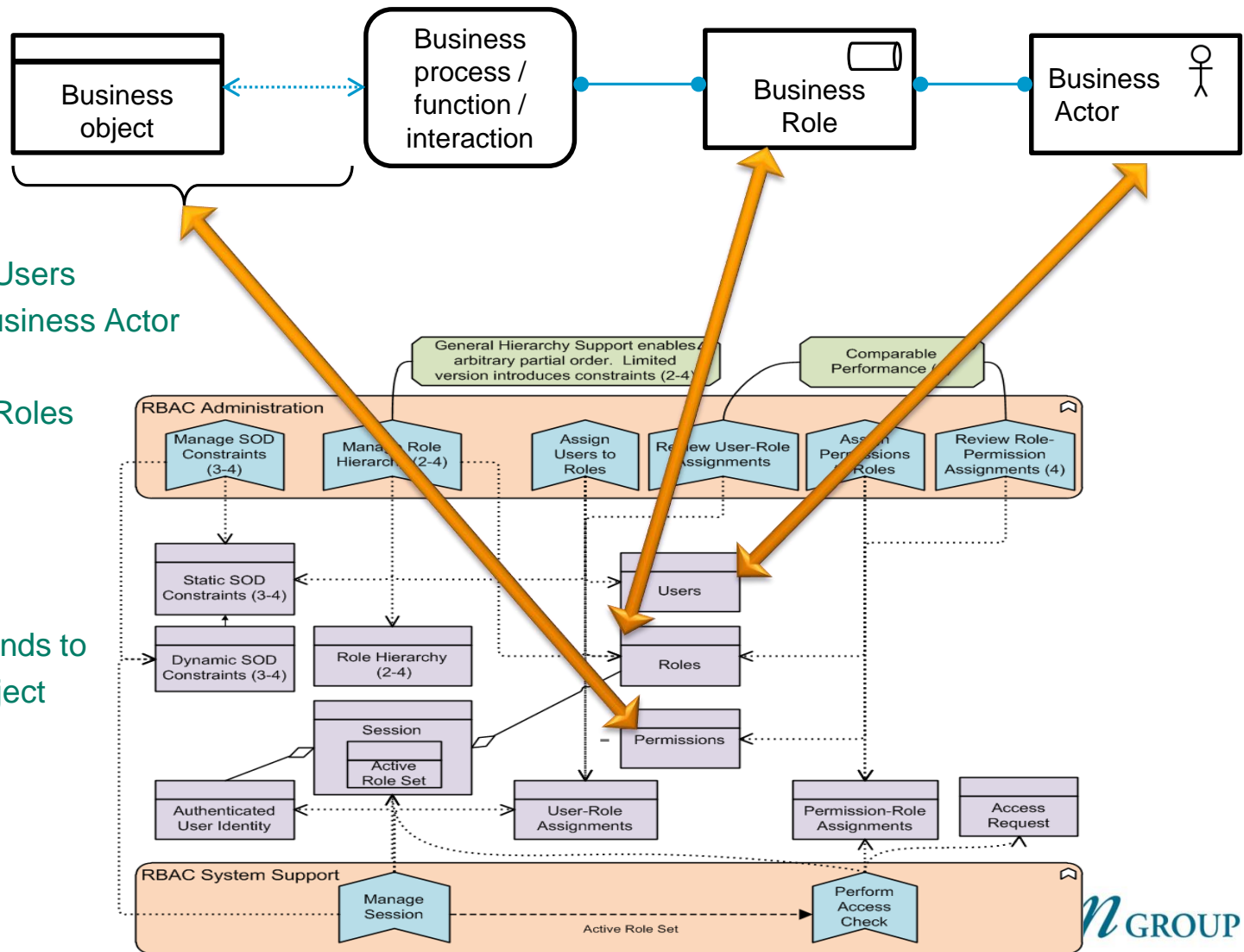
Administration framework

Modeling RBAC with SABSA, TOGAF and
ArchiMate, Creating a Foundation for
Understanding and Action,
Iver Band, CISSP
Open Group Conference, Austin, Texas

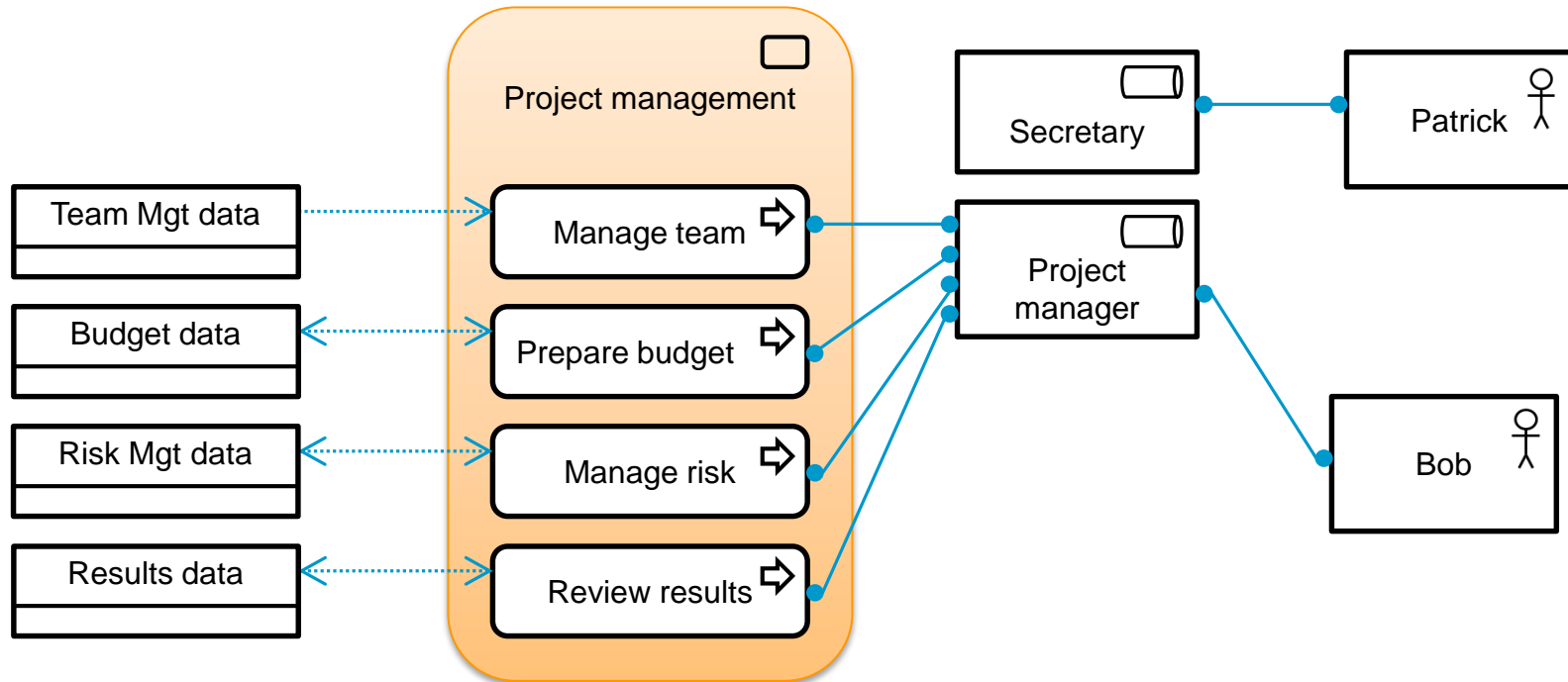
- The *data object* Users corresponds to the Business Actor

- The *data object* Roles corresponds to the Business Role

- The *data object* Permissions corresponds to the access to data object

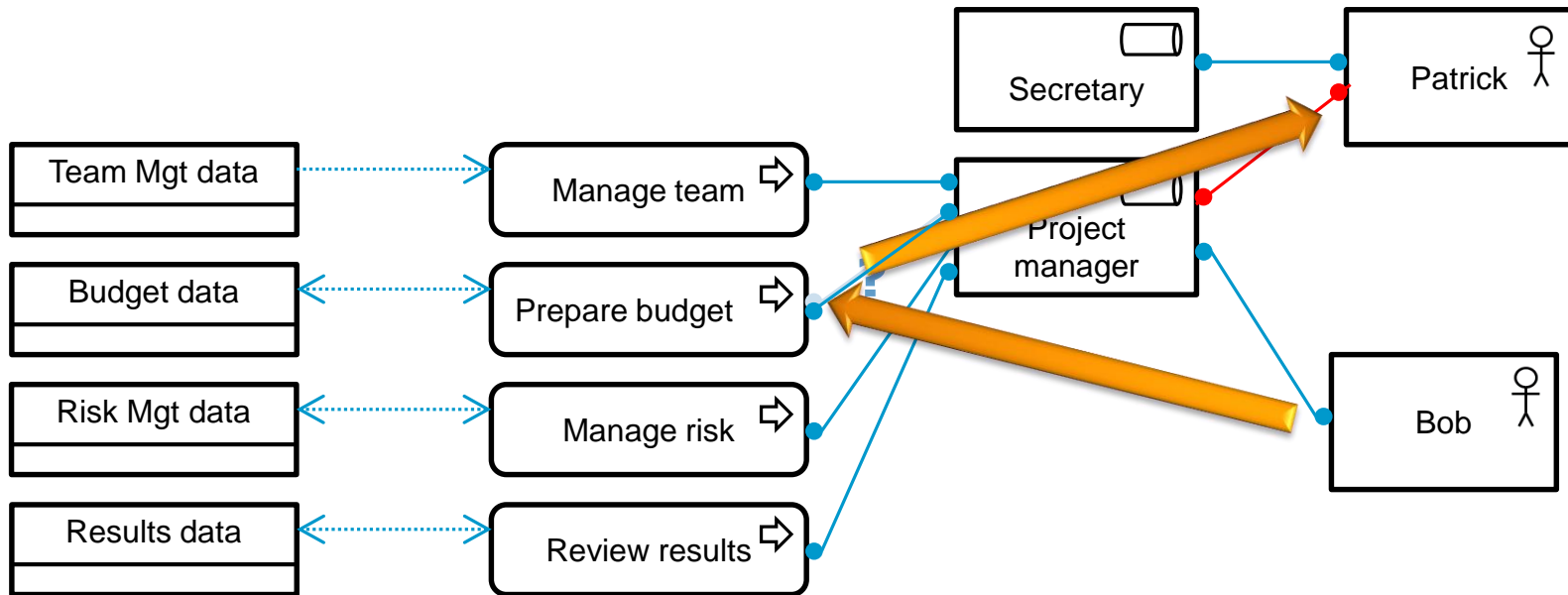


Case study



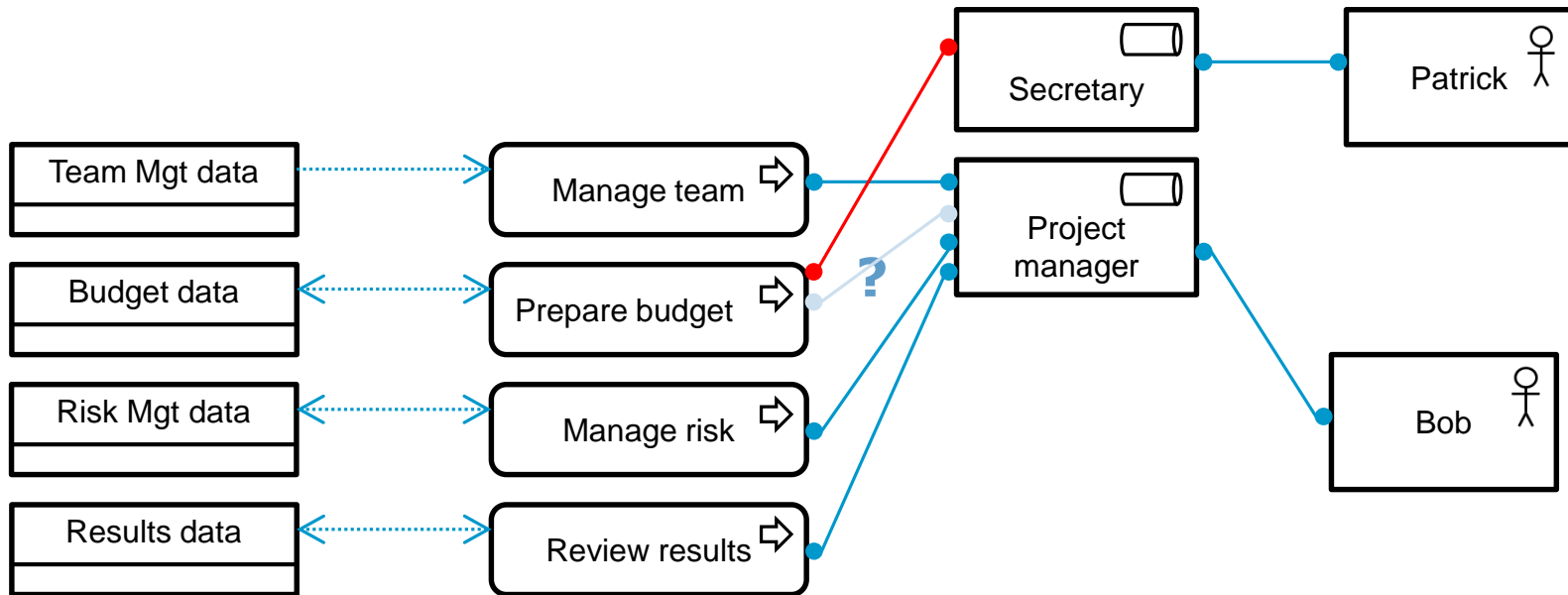
- The role of project manager is assigned to four processes that compose the project management service
- Each of these processes **accesses specific data**
- Bob is a project manager

Case study



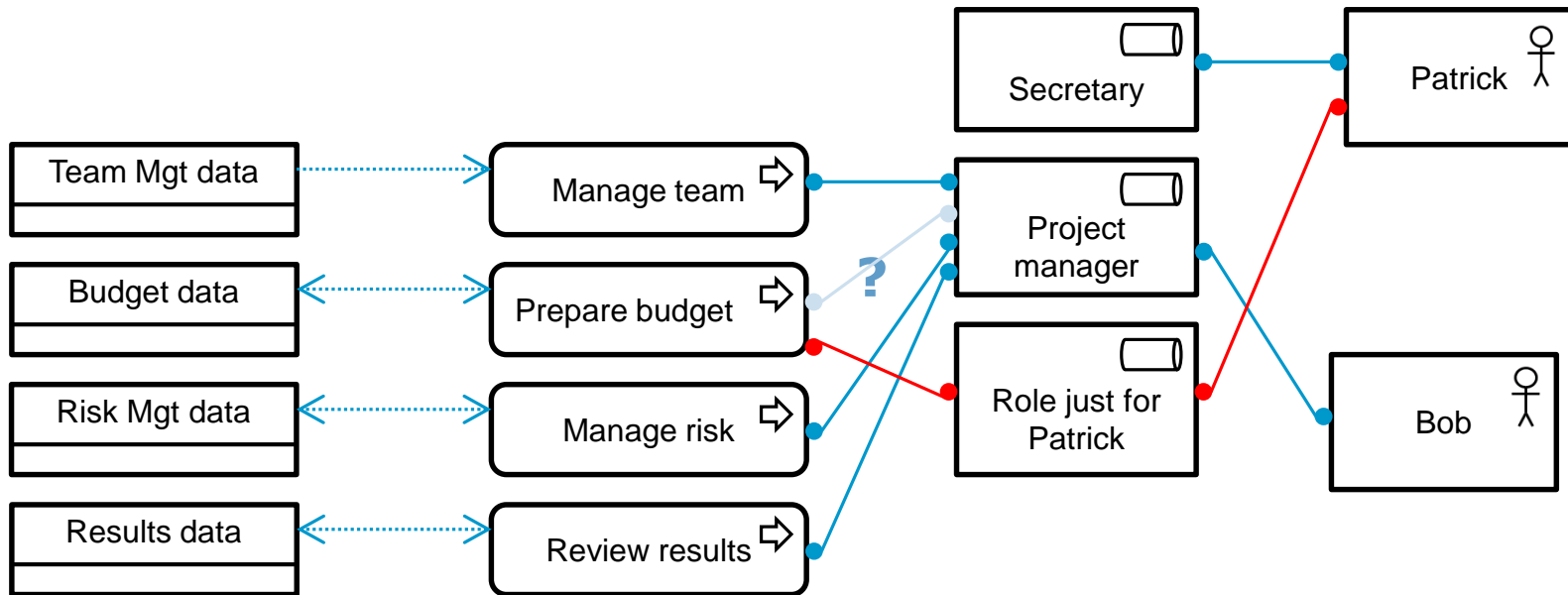
- Bob has too much work and delegates the preparation of the budget to his secretary, Patrick.
- → How can Bob assign Patrick the necessary rights?

Case study



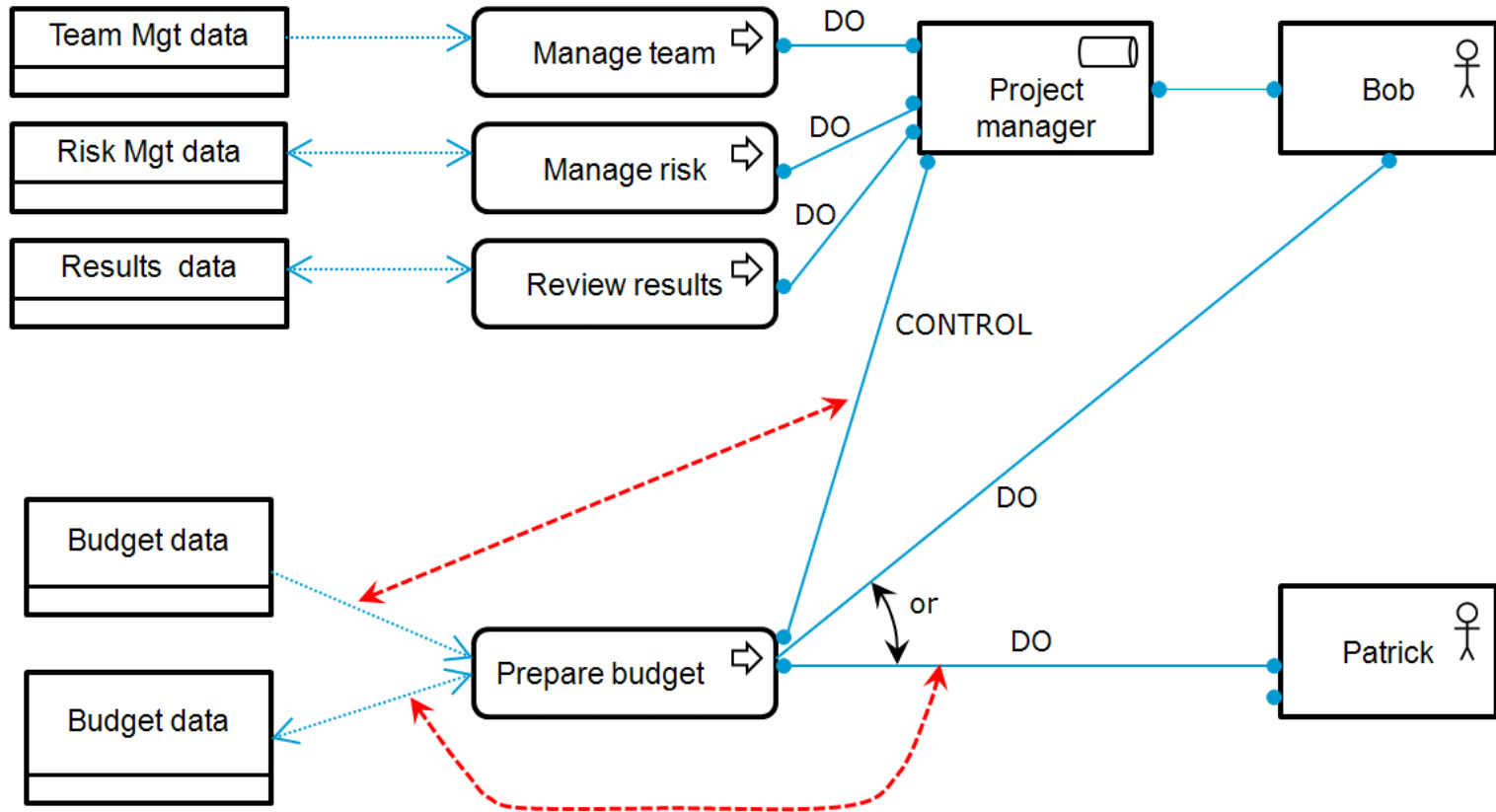
- In this model, the Secretary role is assigned to the Prepare Budget Process
- What happens to the other secretaries?
→ They receive too many rights

Case study



- In this model, Patrick gets a special-purpose role
- Is Patrick the only person who can manage the budget ?

What we need to model



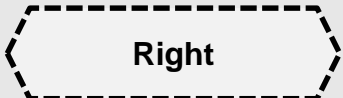
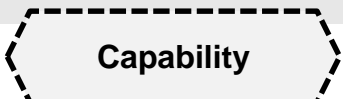
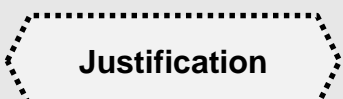


Therefore, we introduce **RESPONSIBILITY**

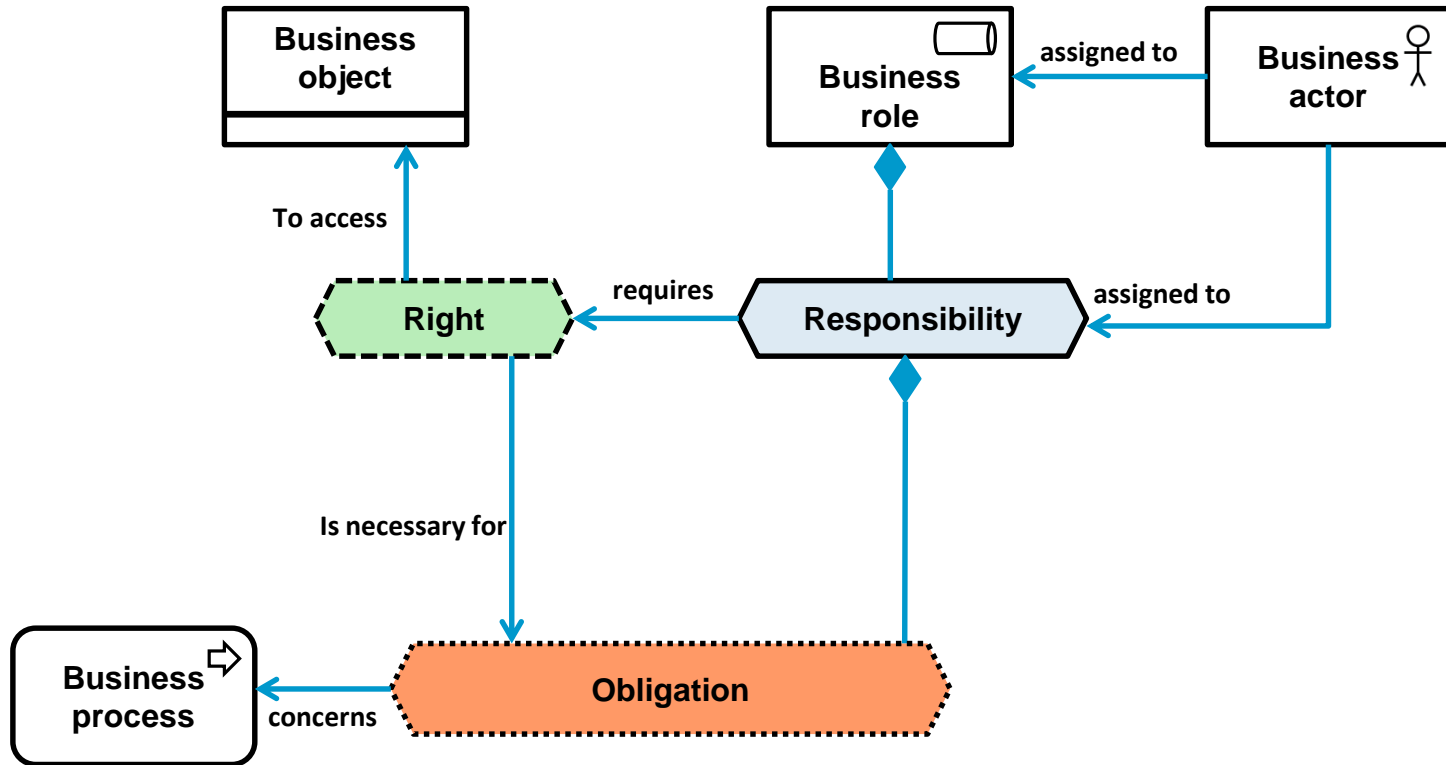
Responsibility Modeling

- How should responsibility be modelled, both in general and specifically in ArchiMate ?
 - New concepts
 - Relation between those concepts and ArchiMate
 - Illustrations with the case study

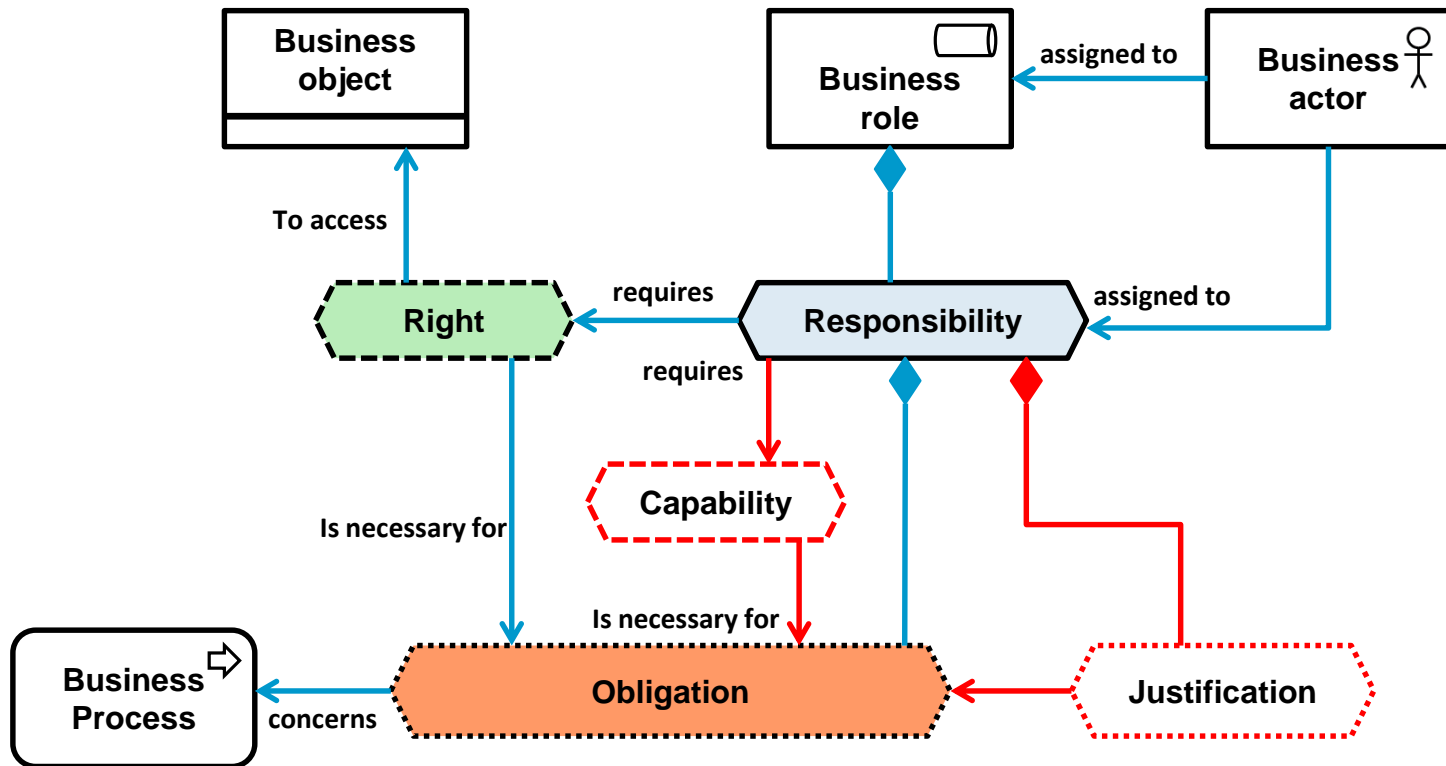
New Concepts

Name	Symbol	Meaning
Responsibility		A property assigned to a business actor that aggregates a set of obligations and rights
Obligation		An obligation is a duty to perform a task
Right		An ability granted to a business actor by the enterprise in order to enable the business actor to perform a specific task.
Capability		An ability of a business actor that has not been granted by the enterprise.
Justification		A justification is a duty to report and explain the action to a given authority

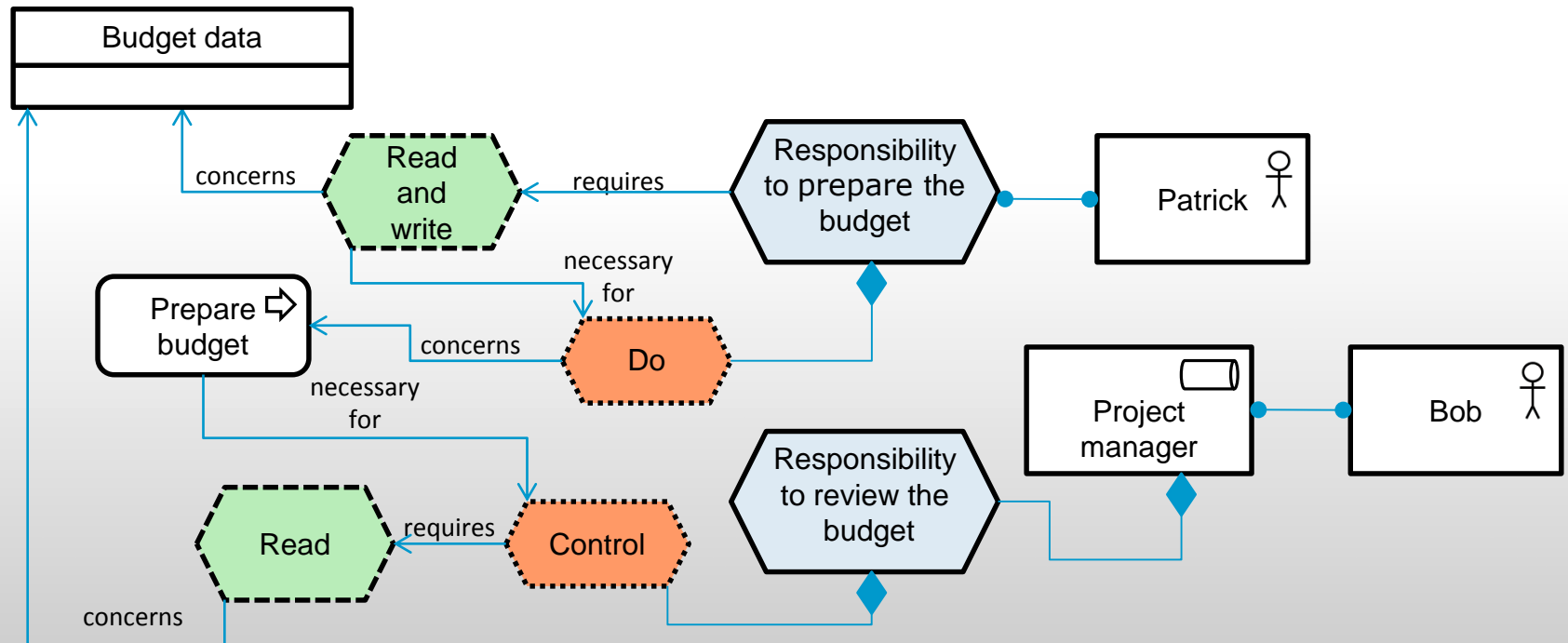
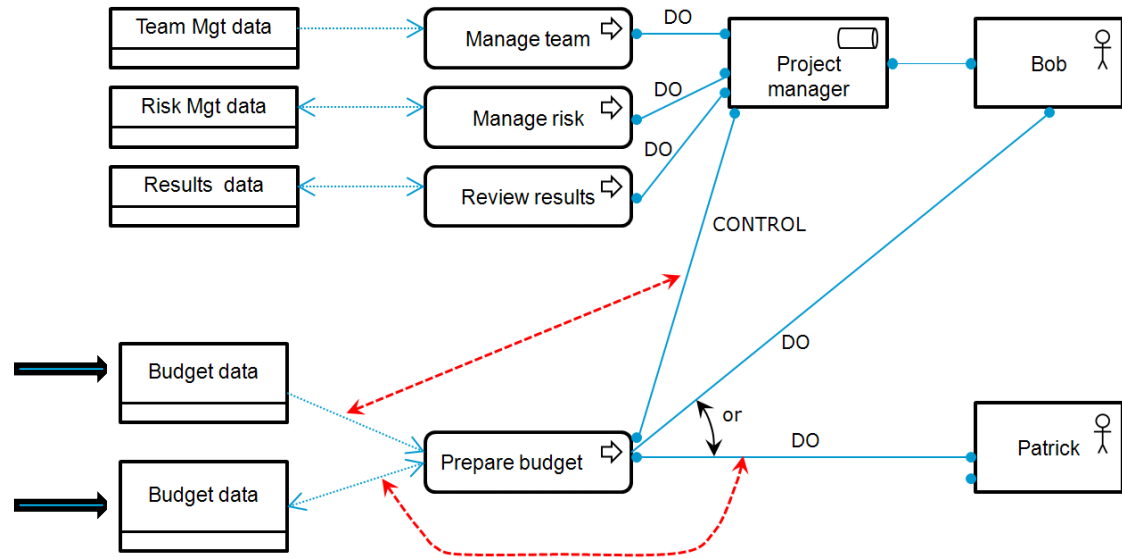
Responsibility Modeling



Responsibility Modeling



Responsibilities to perform and control the budget



Outline

- Context of the research
 - The problem / the research approach
 - What is RBAC ?
 - Case study
- 1st research question: How should responsibility be modelled, both in general and specifically in ArchiMate ?
- 2nd research question: How can models of responsibility be used to improve access rights management ?
- Conclusions

Second research question

- How to include the responsibility with RBAC and with RBAC administration framework ?
 - Introduction of the responsibility at the business layer and at the application layer
 - Association of the responsibility with the Business role and the RBAC role.
 - Illustration with the case study

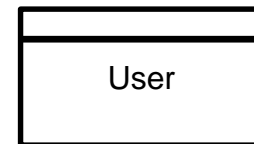
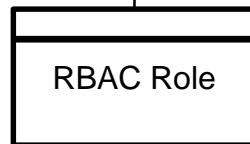
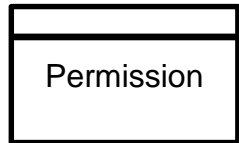
Administrative Framework **without** Responsibility

Business Layer



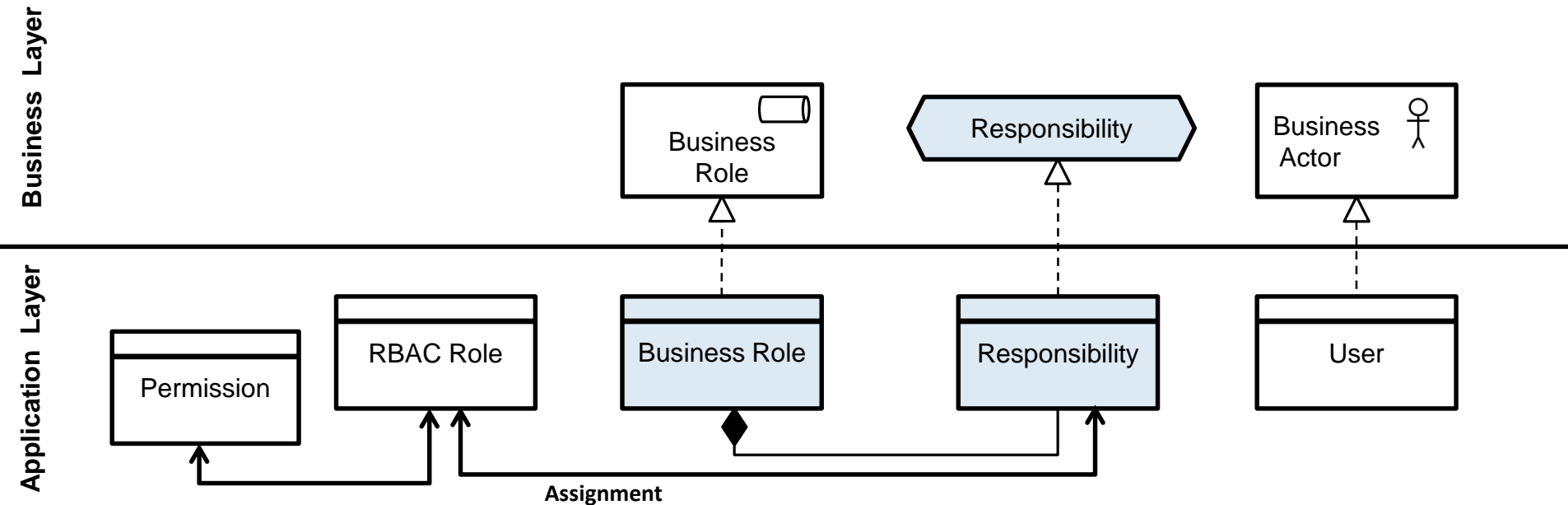
Application Layer

Inappropriate !

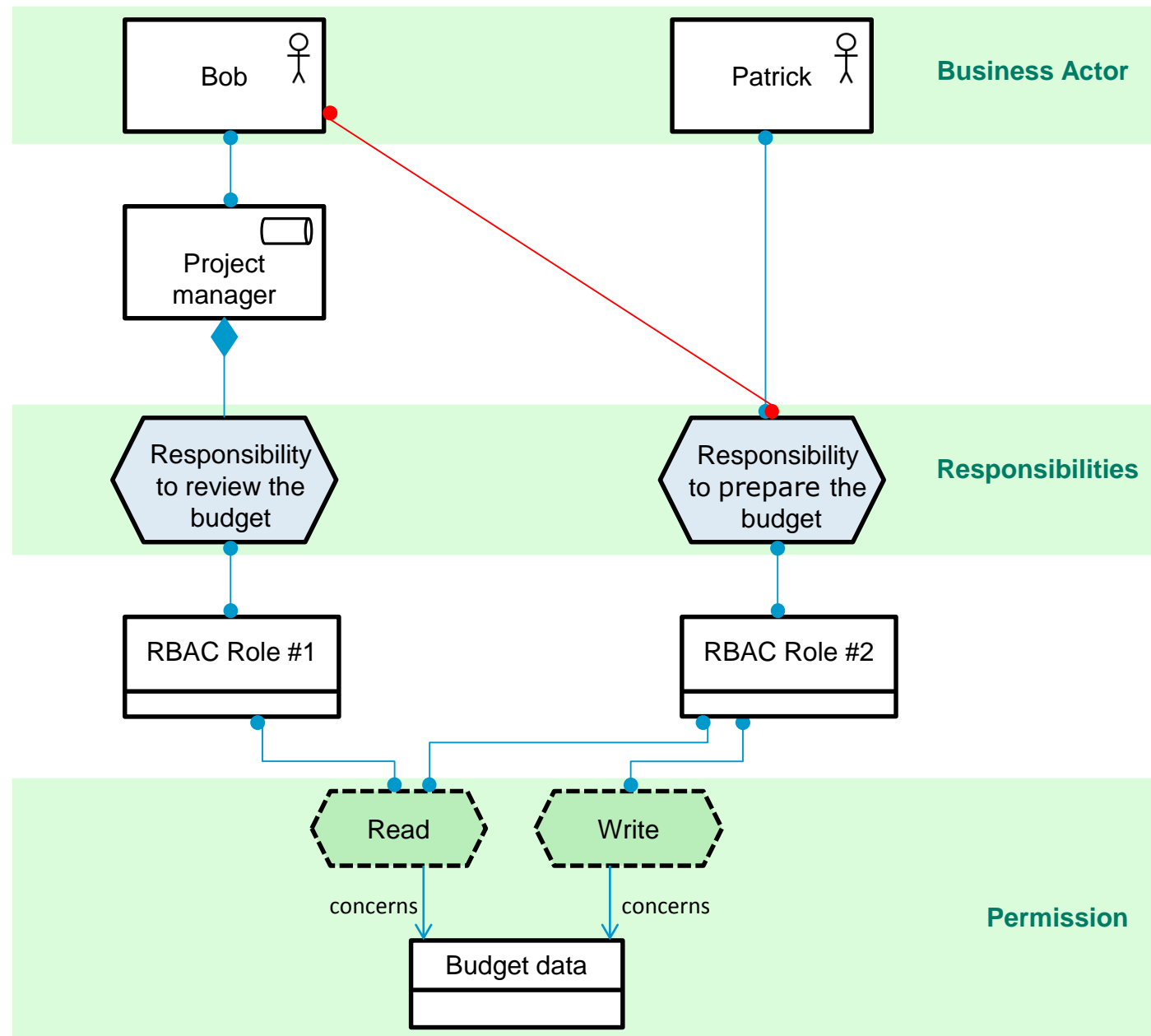


Assignment

Administrative Framework **with** Responsibility

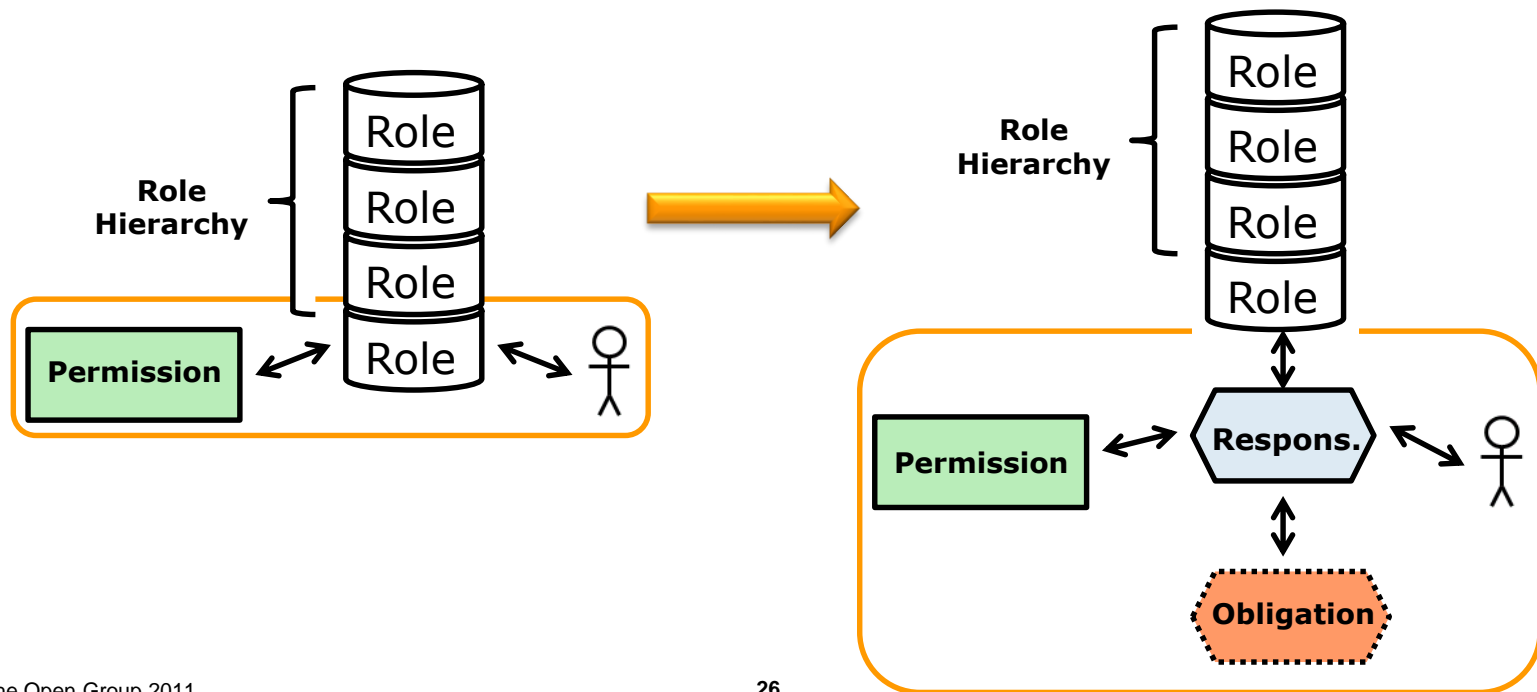


Case Study with Responsibility



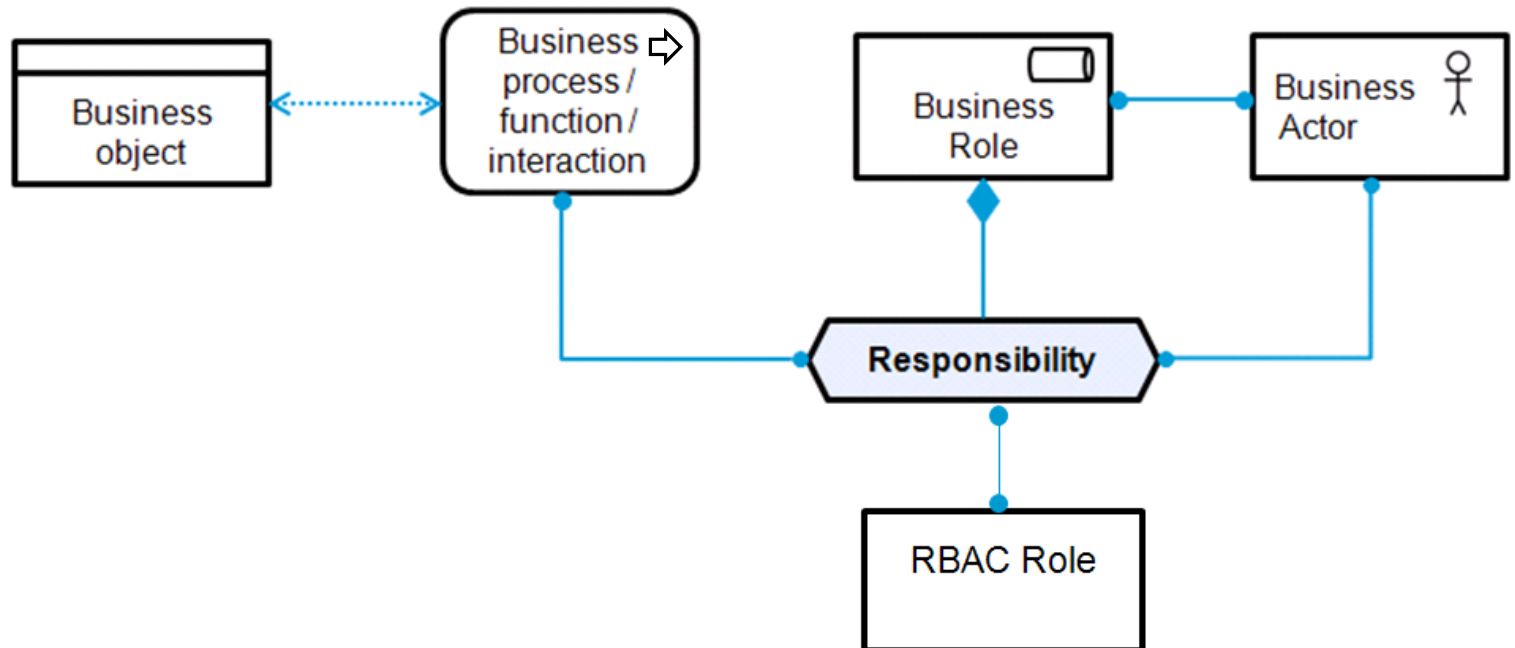
Conclusion

- In order to meet security and governance requirements, enterprises must precisely define responsibilities and provision access rights
- The proposed responsibility extension to ArchiMate enables this precision



Conclusion

- The **responsibility** concept aligns access rights between the ArchiMate Business and Application layers.



Motivation: The *Inaction* Problem in Information Security

Stakeholder Inaction Causes Great Harm

- According to an international study of 761 data compromise incidents in 2010¹
 - 83% of victims were targets of opportunity, the same as 2009
 - 92% of attacks were not highly difficult, up 7% from 2009
 - 96% of breaches were avoidable through simple or intermediate controls, the same as 2009
 - 89% of victims subject to the Payment Card Industry Data Security Standard² had not achieved compliance

Why Don't Stakeholders Act?

- Economic explanations fall into categories such as³
 - Misaligned incentives
 - Breach victims often suffer more than individuals responsible for preventing breaches
 - Employees are often more motivated to do things quickly and cheaply than securely
 - Asymmetric information
 - Market participants are variously incited to exaggerate or minimize risk
 - Exaggerated claims about premium countermeasures make customers unwilling to pay extra for better security
 - Network Externalities
 - Embracing weak security often helps build market share
 - Early countermeasure adopters must often await broader adoption to realize benefits
 - Externalities of Insecurity
 - The social cost of asset compromise is often greater than the owners' cost

Why Don't Stakeholders Act?

- Security measures are always trade-offs, but our innate psychology causes us to misinterpret risk. Bruce Schneier⁴ identifies five areas that we often get wrong
 - Risk severity
 - Risk probability
 - Risk impact
 - Effectiveness of countermeasures
 - Comparison of disparate risks and costs
- For example, we often⁴
 - Exaggerate spectacular but rare risks and downplay common ones
 - Have trouble estimating risks for anything outside our normal situation
 - Perceive personified risks as greater than anonymous risks
 - Underestimate risks we willingly take or have some control over, but overestimate risks we can't control
 - Overestimate risks that are receiving great publicity, that are new, or are man-made relative to risks that are less publicized, commonplace or natural in origin

Why Don't Stakeholders Act?

- We are much better equipped to address imminent threats versus those looming in the distance. As Schneier⁴ says
 - *“We are very well adapted to dealing with the security environment endemic to hominids living in small family groups on the highland plains of East Africa”*
- In fact, our “Abstract concepts are largely metaphorical”⁵. For example, we
 - *Punch a hole* in the firewall
 - Experience security *breaches*
 - Analyze attack *surfaces*
 - All too often, end up between a *rock and a hard place*

Questions for Discussion

- How can security architects use the ArchiMate visual modeling language to
 - Align stakeholders' *perceptions* of risk with the logical and mathematical *reality* of enterprise risk?
 - Enable the sponsors, designers and implementers of controls to make the best possible protective decisions for their enterprise?
- How can The Open Group build on ArchiMate 2.0 to better support security architecture?

Thank You!

Supplementary Material

Motivation References

1. **W. Baker, A. Hutton, C.D. Hylender, J. Pamula, C. Porter, M. Spitler, et. al.** 2011 Data Breach Investigations Report [Online], 2011.
http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
2. **PCI Security Standards Council.** Payment Card Industry Data Security Standard version 2.0 [Online], 2010.
https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0
3. **T. Moore, R. Anderson.** Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research [Online], 2011.
<ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf>
4. **B. Schneier.** The Psychology of Security [Online], 2008.
<http://www.schneier.com/essay-155.html>
5. **Lakoff, George, Johnson, Mark.** *Philosophy in the Flesh.* Basic Books, 1999.

Responsibility References

1. **Christophe Feltus, Eric Dubois, Erik Proper, Iver Band, Michaël Petit**, Enhancing the ArchiMate® Standard with a Responsibility Modeling Language for Access Rights Management, 5th ACM International Conference on Security of Information and Networks (ACM SIN 2012), 22-27/10/2012, Jaipur, Rajasthan, India. ISBN: 978-1-4503-1668-2
2. **Christophe Feltus, Michaël Petit, Eric Dubois**, ReMoLa: Responsibility Model Language to Align Access Rights with Business Process Requirements, Fifth IEEE International Conference on Research Challenges in Information Science (IEEE RCIS 2011), 19-21/5/2011, Guadeloupe - French West Indies, France
3. **Christophe Feltus, Eric Dubois, Michaël Petit**, *Conceptualizing a Responsibility based Approach for Elaborating and Verifying RBAC Policies Conforming with CobiT Framework Requirements*, Third International Workshop on Requirements Engineering and Law (RELAW10), in conjunction with the 18th IEEE International Requirements Engineering Conference (RE2010), 27/9-1/10/2010, Sydney, Australia.
4. **Christophe Feltus, Michaël Petit, Morris Sloman**, *Enhancement of Business IT Alignment by Including Responsibility Components in RBAC*, 5th International Workshop on Business/IT Alignment and Interoperability (BUSITAL 2010), an International Workshop of the 22th Conference on Advanced Information Systems Engineering (CAISE2010), 7-11/6/2010, Hammamet, Tunisia
5. **Christophe Feltus, Michaël Petit, Eric Dubois**, *Strengthening Employee's Responsibility to Enhance Governance of IT - COBIT RACI Chart Case Study*, The 1st ACM Workshop on Information Security Governance (ACM WISG 2009) held in conjunction with the 16th ACM Conference on Computer and Communications Security (ACM CCS 2009), 13/11/2009, Chicago, Illinois, USA.
6. **Christophe Feltus, Michaël Petit**, Building a Responsibility Model Including Accountability, Capability and Commitment, Fourth International Conference on Availability, Reliability and Security ("ARES 2009 – The International Dependability Conference") IEEE, 16-19/3/2009, Fukuoka, Japan. (SCOPUS)
7. **Christophe Feltus, Michaël Petit**, Building a Responsibility Model using Modal Logic - Towards Accountability, Capability and Commitment Concepts, The seventh ACS/IEEE International Conference on Computer Systems and Applications (AICCSA-09) IEEE, 10-13/5/2009, Rabat, Morocco